

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

公開情報: (n, E)
 検証器を特権化する情報: (ν, δ)
 入力: μ
 出力: M または *invalid*

検証器

```

C := rand
send (C, n)
receive  $\chi$ 
 $\rho := (\chi || \mu)^\delta \bmod \nu$ 
send  $\rho$ 
receive R
if  $R^E \bmod n = C || M$ 
  output M
else
  output invalid

```

証明器

```

receive (C, n)
find  $(n, t, L)$ 
 $f || \nu || c || P_0 || P_1 || P_2 || P_3 || P_4 || P_5 := L$ 
if f
   $\chi := \text{rand}$ 
  send  $\chi$ 
  receive  $\rho$ 
  if  $\rho^\delta \bmod \nu = \chi || \mu$ 
    M := 0
    P0
  else
    M := 1
    P1
    P2
    if P3
      P4
      R :=  $(C || M)^D \bmod n$ 
    else
      P5
      R := undefind
  send R

```

【0212】[2.15. 第13の対話プロトコル]
 (検証器3の構成、図30) この発明における第13の検証プロトコルでは、検証器3の特権を与える特徴情報をチケットとして与え、検証器3の特権保証特徴情報による符号化は前述までのチケット証明器2と同様に与える。

【0213】図30はこの検証プロトコルを行なう検証器3の構成図である。

【0214】検証器3は特権を保証する秘密情報 δ による符号化を行なう場合、チケット保持部114から対応するチケットを取りだし、固有情報保持部113に保持

40 された固有情報を基に符号化する。

【0215】[3. 第2の実施例]

[3.1. 認証手法] 本実施例では、チケットの特徴情報は、以下の形で与えられる。

【0216】 p は素数であり、 G は離散対数問題が困難な有限群であり、 g は有限群 G の位数 p の元であり、 $y = g^x$ が満たされるとき、 (p, G, g, y, x) がチケットの特徴情報である。特に、 (p, G, g, y) を公開の特徴情報とし、 y を秘密の特徴情報とする場合について、実現できるチケットの証明方法について詳述する。

【0217】実際には、 G を有限体の乗法群として構成したり、有限体上の楕円曲線として構成することができる。

【0218】例えば、 (p, G, g) をシステム共通とし、公開情報 y 、秘密情報 x とする。チケットはチケット特徴情報 x と証明器固有情報 d_u とチケット付加情報 L より計算されるデータであり、証明器2が (C, y, t, L) に対して証明器固有情報 d_u を用いて $\tau(C, y, t, L) = C^*$ が計算できるように構成する。

【0219】例えば、 d_u をある暗号系の復号鍵とし、 E_u を d_u に対応する暗号化とし、 H を一方方向性関数としたとき、 $t := (E_u(x), H(d_u || x || L))$ のように定めることができる。

【0220】チケットを上述の様に定義すると、チケットを用いた秘密の特徴情報 x による符号化 C^* は、入力 (C, y, t, L) に対して証明器2の固有情報 d_u によって $E_u(D)$ を復号して証明器2中で D を回復し、その値を用いて一方方向性関数の値をチケットと比較することによって L の値の正当性を確認し、回復された D の値を用いて証明器2内で C^* を計算するようにすれば良い。

【0221】また、 d_u を一方方向性関数として、 $t = x - d_u(L, y)$ と定めることもできる。

【0222】チケットの上述の定義によれば、入力 (C, y, t, L) に対して D による符号化は $C^* = C^{d_u(L, y)}$ を計算することによって行なうこともできる。

【0223】まずは離散対数問題の困難さに安全性の根拠をおく、秘密値共有の原理を利用した対話プロトコルの例を挙げる。

【0224】〔3.2.第14の対話プロトコル〕
(証明器2が時計を持つ定期券型のチケット、図13、図19、図20)第14の対話プロトコルでは、証明器2の内部状態として時計情報を持っているとする。本プロトコルにおける検証器3の手順を図13に、証明器2の手順を図19に従って説明する。

【0225】検証器3は、認証情報生成部286によって乱数 r を生成して、 $C := g^r$ としてチャレンジ C を生成して、認証情報保持部287に記録する(ステップ131)。ステップ132の代わりに、認証情報保持部287に記録された C と、公開情報 y をまとめて、送信部281より証明器2へ送信する。

【0226】ステップ191の代わりに、証明器2は、検証器3から送信された (C, y) を受信部292で受信して、情報保持部299に記録する。チケット探索部122は受信した y に対応するチケットをチケット保持部121から探して、チケットを持っているかどうかを判定する(ステップ192)。レスポンス R にチケットを持たないことを意味する値(この場合は0)を設定して、情報保持部299に記録する(ステップ197)。

ステップ192の判定の結果として対応するチケットを持つ場合には、チケット t 、証明器2の手順Provers、チケット付加情報 L を制御部2912内にセットする(ステップ193)。

【0227】ステップ193が実行されたら、ステップ194を実行する。この対話の例におけるステップ194の詳細な手順を図20に従って説明する。内部状態保持部124の第2の内部状態保持部から読み出したその時の時刻 $time$ と、 L に記述されている有効期限とを比較して、チケットがその時点で有効であるか判定する(ステップ201)。チケットを有効であると判定した場合には、第1の演算部293において R を、 $R := C^*$ のように計算して、情報保持部299に記録する(ステップ202)。特に R のこの計算を、証明器2の中の第1の演算部293ですべて計算してもよいが、チケット t が $t = x - d_u(L, y)$ のように構成されている場合には、 C^* の計算は $C^* = C^{d_u(L, y)}$ のようにも計算できるので、 C^* を証明器2の外で計算して、証明器2の中の第1の演算部293で計算した $C^{d_u(L, y)}$ とを証明器2の外で掛け合わせても計算できる。証明器2の計算速度が遅い場合には、このような方法も有効になる。ステップ201においてチケットを無効であると判定した場合には、必要であるならばチケットをチケット保持部121から削除して(ステップ203)、 R に1を設定して、情報保持部299に記録する(ステップ204)。ここまでの対話の例におけるステップ194の詳細な手順である。

【0228】ステップ194が実行されたら、ステップ193でセットされた t 、Provers、 L を制御部2912から解除する(ステップ195)。ステップ195もしくはステップ197が実行されたら、 R を送信部291より検証器3へ送信する(ステップ196)。

【0229】検証器3は、受信部282において証明器2から送信された R を受信して、情報保持部289に記録する(ステップ133)。 y^r を第1の演算部283で計算して、その計算結果が R と一致するかを、正当性検証部285で判定する(ステップ134)。一致すると判定された場合は証明器2が有効なチケットを持っていることを示すので、「有効」を意味する出力を出力部2812より出力する。一致しないと判定された場合は証明器2が有効なチケットを持っていることが示されなかったため、「無効」を意味する出力を出力部2812より出力する。

【0230】以上が第14の対話プロトコルである。第14のプロトコルでは、最初の簡単なプロトコルと同様の機能を提供している。

【0231】

〔表13〕

61

検証器公開情報: y

出力: '有効' もしくは '無効'

 $r := \text{rand}$ $C := g^r$ send (C, y)receive R if $y^r = R$

output '有効'

else

output '無効'

Proverif time $< L$ $R = C^y$

else

 $R = 1$

【0232】 [3.3. 第15の対話プロトコル]
 (使い捨て型の回数券型のチケット、図19、図32、
 図33) 第15の対話プロトコルで利用するチケット補
 助情報Lには、検証器3の公開情報 η と、カウンタ i 、
 の上限値 i が含まれていることを前提にする。第15の
 対話プロトコルにおける検証器3の手順を図32に、証
 明器2の手順を図19にそれぞれ従って説明する。

【0233】 検証器3は、認証情報生成部286によっ
 て乱数 r を生成して、 $C := g^r$ としてチャレンジ C を
 生成して、認証情報保持部287に記録する(ステップ
 321)。認証情報保持部287に記録された C と、公
 開情報 y をまとめて、送信部281より証明器2へ送信
 する(ステップ322)。

【0234】 ステップ191の代わりに、証明器2は、
 検証器3から送信された(C, y)を受信部292で受
 信して、情報保持部299に記録する。チケット探索部
 122は受信した y に対応するチケットをチケット保持
 部121から探して、チケットを持っているかどうかを
 判定する(ステップ192)。対応するチケットを持た
 ない場合には、レスポンス R に0を設定して、情報保持
 部299に記録する(ステップ197)。対応するチケ
 ットを持つ場合には、チケット t 、証明器2の手順Pr
 over s 、チケット付加情報 L をセットする(ステッ
 プ193)。Prover s のセットとして、 L より
 (η, i)を取り出しておく。

【0235】 ステップ193が実行されたら、ステップ
 194を実行する。本プロトコルにおけるステップ19
 4の詳細な手順を図33に従って説明する。認証情報生
 成部296チャレンジで乱数 s を生成して、 $\chi := g^s$
 としてチャレンジ χ を生成して、第2の認証情報保持部

62

298に記録する(ステップ331)。送信部291から
 検証器2に χ を送信する(ステップ332)。

【0236】 検証器3は、 χ を受信部282で受信し
 て、情報保持部289に記録する(ステップ323)。
 受信した χ が0の場合は、チケットが無くて R が0とし
 て送られたことを示すので、「無効」意味する出力を出
 力部2812より出力して、対話プロトコルを終了する
 (ステップ324)。第2の演算部284においてレス
 ポンス ρ を、

【0237】
 【数35】

$$\rho := \chi^r$$

として計算する(ステップ325)。計算した ρ を送信
 部281より証明器2へ送信する(ステップ326)。

【0238】 証明器2は、 ρ を受信部292で受信し
 て、情報保持部299に記録する(ステップ333)。
 第2の演算部294で η^* を計算して、受信した ρ と一
 致するか判定する(ステップ334)。判定の結果とし
 て一致する場合には、内部状態保持部124の第2の内
 部状態保持部に確保されているカウンタ i の値をイン
 クリメントする(ステップ335)。ステップ335が
 実行されたら、 i の値を L より得られた上限値 i と比
 較する(ステップ336)。ステップ337の比較の結果
 として、 i の値が i 以下の場合には、第1の演算部2
 93で $R := C^*$ を計算して、情報保持部299に記録
 する(ステップ337)。ステップ337の比較の結果
 として、 i の値が i より大きい場合は、内部状態保持
 部124の第2の内部状態保持部から i を解放して、
 チケット保持部121からチケットを削除して(ステッ
 プ338)。ステップ334で一致しなかった場合と合

わせてRに1を設定して、情報保持部299に記録する(ステップ339)。ここまでが第15の対話プロトコルにおけるステップ194の詳細な手順である。

【0239】ステップ194が実行されたら、ステップ193でセットされた t 、 $Provers$ 、 L を解除する(ステップ195)。ステップ195もしくはステップ197が実行されたら、送信部291から検証器3へRを送信する(ステップ196)。

【0240】検証器3は、受信部282において証明器2から送信されたRを受信して、情報保持部289に記録する(ステップ327)。 y^r を第1の演算部283で計算して、その計算結果がRと一致するかを、正当性*

検証器

```

r := rand
C := gr
send (C, y)
receive x
ρ := xε
receive R
if yr = R
    output '有効'
else
    output '無効'

```

Prover

```

s = rand
χ := gs
send χ
receive ρ
if ηs = ρ
    i := i + 1
    R = C*
else
    R = 1

```

【0243】[4. 第3の実施例]

(チケットの初期化、図5～図12) この第3の実施例において、チケット作成・発行装置1とチケット証明器2は、チケットの多重初期化を回避するために、チケット

【0244】チケット作成・発行装置1においては、チケットカウント手段は証明器固有情報保持手段(データベース)7に含ませる構成にしても構わない。また、チケット証明器2においては、チケットカウント手段は内容の書換えが行なえないような防御機構を設けてあればより適切である。

【0245】なお、チケット作成・発行装置1によるチケット作成・発行の全体の動作については第4の実施例を参照して後に詳述する。

*検証部285で判定する(ステップ328)。一致すると判定された場合は証明器2が有効なチケットを持っていることを示すので、「有効」を意味する出力を出力部2812より出力する。一致しないと判定された場合は証明器2が有効なチケットを持っていることが示されなかったので、「無効」を意味する出力を出力部2812より出力する。

【0241】以上が第15の対話プロトコルである。本プロトコルは、第1の実施例の第3の対話プロトコルと同様の機能を提供する。

【0242】

【表14】

【0246】チケット発行の手順を図5を参照して説明する。図5において、チケット発行時、ステップ55において、そのチケットが証明器2内部の状態を初期化すると判定されれば、チケット作成・発行装置1のチケットカウント手段からカウンタ値を取り出してチケットと共に送る。初期化が不要な場合は $i = 0$ を送る。チケットカウンタ値は最初に1に設定されている。ステップ56においては次回のチケット発行要求に備えるためにカウンタ値を1増加する。チケットは公開情報だが完全性を保つ必要はある。したがって、センターが署名手段を持ち、証明器識別子とカウンタ値とチケット識別子と初期化手順と証明手順とチケット付加情報とに署名を施すのは好適である。

【0247】図6は、発行されたチケットの証明器2へ

の登録を行なう手順を表している。図6において、ステップ61でチケット保持部に余裕があることを確認し、ステップ62でチケットへの署名の検証を行なう。ステップ63で証明器識別子が正しいことを確認し、ステップ64で*i*の値により初期化が必要かどうかを判定する。初期化が必要と判定されるとステップ65で*i*の値が初期化に必要なチケットとしてはじめて現れたかどうかを判定する。

【0248】この判定の手順は図7で説明される。はじめてのチケット登録と判定されればステップ66で初期化が実行される。初期化の実行例は図8および図9で例を挙げて説明する。初期化が不要な場合はチケット保持手段に入力されたチケットを登録する。

【0249】図7は、内部状態多重初期化回避の判定を行なう手順を表している。ここでは、証明器2の内部状態保持手段には通し番号のリストを保持する手段を設ける構成として説明する。

【0250】チケットカウント手段に保持された*i*₀は、今までに初期化が行なわれたチケットの通し番号*i*のうち最大のものであり、内部状態保持手段に保持されたリストは*i*₀より小さい通し番号のうち未だ初期化されていないものからなる。

【0251】入力された通し番号*i*に対して、まずステップ71でチケットカウント手段に保持された*i*₀との比較を行なう。*i* > *i*₀であれば通し番号*i*に対応する初期化はまだ行なわれていないので、ステップ72へ進み、そうでないならばステップ74へ進む。ステップ72では、*i*₀より大きく*i*より小さい初期化が未だ行なわれていない通し番号をリストに加える。もしも、リストに加えることができなければリストのオーバーフローなので例外処理を行なう。ついでステップ73では、*i*₀の値を*i*で置き換えて、OKを出力する。

【0252】ステップ74では、*i*が内部状態保持手段に保持されたリストに存在するかどうかを判定する。リストにあれば、ステップ75で*i*をリストから削除し、OKを出力する。リストになれば、NGを出力する。

【0253】図8と図9はチケットに対する内部状態の初期化の手順を表している。図8および図9において、まず、ステップ81、91で初期化の領域確保が可能かどうか判断し、可能であれば、ステップ82または92において内部状態*i*₀をゼロまたはLに初期化する。

【0254】また、証明器2からのチケットの削除は図10に示すようにパスワードによる認証で行うことができる。また内部状態の開放も図11に示すように同様にパスワードによる認証で行うことができる。

【0255】〔第4の実施例〕

(チケット作成・発行装置1のチケット作成・発行、図2、図3、図4、図5) 第4の実施例としてチケット作成・発行装置1を説明する。図4はチケット作成の手順を示している。

【0256】チケット作成手段4は、チケットの仕様を指示したチケット作成依頼を受け取る。ここでチケットの仕様とは、チケットの検証手順と証明手順と初期化手順とチケット付加情報のデータの型とチケット発行依頼者の資格情報とからなる。

【0257】手順の指定には手順に対する識別子を用意して、その識別子で指示しても良いし、手順自体を与えるようにしても良い。以下では、仕様の識別子によって指定する方法を述べる。また、チケットが内部状態を持ち、特権を持つ検証者とその内部状態を変更できる場合は、検証手順と証明手順を決定するためには、検証者の特権に対応する証明証も与える必要がある。

【0258】図4において、チケット作成手段は、チケット作成依頼を受けるとステップ41において仕様を検索する。ついで、ステップ42においてチケットの特徴情報を生成する。ここでは、RSA公開鍵暗号系の公開鍵ペアを特徴情報とするものとする。チケットの特徴情報はチケットの作成依頼に応じて作成しても良いし、予め作成して用意しておいても良い。ステップ43において特徴情報と仕様の識別子とチケット付加情報のデータの型とチケット発行依頼者の資格情報(と必要ならば特権を持つ検証者の証明証)の組をチケット原型データベース6に記憶する。ステップ44においてチケット識別子*n*とチケット公開情報*E*とチケット仕様*S*に対応するチケット検証手順*Verifiers*に対して署名を行ない、それをチケット作成依頼者に与える。

【0259】図5はチケット発行の手順を表している。図5において、チケット発行依頼者は、チケット識別子と証明器識別子とチケット仕様識別子とチケット付加情報により、チケットを指定して発行の依頼を行なう。この際、チケット発行手段5はチケット発行依頼者の資格をチケット原型データベースに記憶された資格情報にてらして確かめる。チケット発行手段5は、まず、ステップ51において証明器識別子に対応する固有情報を検索する。ステップ52においてチケット識別子に対応するチケットの原型を検索する。ステップ53において仕様識別子に対応する仕様を検索する。ステップ54において与えられたチケット付加情報の型が正しいかどうかを判定する。ステップ55においてチケットが初期化を伴うかどうかを判定する。チケットが初期化を伴うならば、ステップ56において、証明器固有情報データベース7に記憶された*i*₀を*i*にセットし、ステップ57において*i*₀をインクリメントする。ステップ55においてチケットが初期化を伴わないと判定されれば、ステップ58において*i*を0にセットする。ステップ59において、今までの実施例で述べたように*D*、*d*₀、*L*よりチケット*t*を生成する。ステップ510において証明器識別子*U*と初期化を伴うチケットの通し番号*i*とチケットの初期化手順*Init_s*とチケットの証明手順*Provers*とチケット付加情報*L*とチケット*t*との組にチ

ケット発行手段の署名をつけて発行を行なう。

【0260】

【発明の効果】これまで述べたように、電子チケットを実現するためには、以下の機能を満たす必要がある。第1点は、正当な権利を持たないものが、不当にチケットを利用することを防止する機能である。第2点は、利用者が自分の保持するチケットの正当性を確認できる機能である。第3点は、当事者間で争いが生じたときに備えて、チケットに与えられた権利内容を第三者に証明できる機能である。さらに状況に応じては、第4点として利用者の匿名性が保証される必要がある。

【0261】本発明によれば、複製が非常に困難な証明器とそれに対応するチケットがない限り不正利用が不可能であり、第1の機能を満たす。また、誰が知っている問題のない公開された情報だけで、利用者の持つチケットの内容を証明できるので、第2および第3の機能を満たす。さらに、チケットの検証時に利用者に依存する情報がまったく通信されないので、利用者の匿名性が維持されて、第4の機能を満たす。このように、本発明によれば、以上の4点すべての機能を満たしたチケットの作成・発行・利用システムが実現される。加えて、チケット発行時および検証時の情報の通信をすべて開示できるので、利用者がその内容を確認することで、利用者の権利を侵害する通信が行われていないことを証明する効果も併せ持つ。

【図面の簡単な説明】

【図1】 この発明の原理的な構成例を示すブロック図である。

【図2】 チケット作成・発行装置の構成を示すブロック図である。

【図3】 チケット作成・発行装置の他の構成を示すブロック図である。

【図4】 チケット作成・発行装置の動作を説明するフローチャートである。

【図5】 チケット作成・発行装置の動作を説明するフローチャートである。

【図6】 証明器へのチケット登録の動作を説明するフローチャートである。

【図7】 多重初期化の判定ルーチンを説明するフローチャートである。

【図8】 証明器の内部状態初期化の一例を説明するフローチャートである。

【図9】 証明器の内部状態初期化の一例を説明するフローチャートである。

【図10】 証明器からチケットを削除する手順を説明するフローチャートである。

【図11】 証明器から内部状態を開放する手順を説明するフローチャートである。

【図12】 チケット検証器およびチケット証明器の構成を示すブロック図である。

【図13】 チケット検証の手順を説明するフローチャートである。

【図14】 チケット検証の手順を説明するフローチャートである。

【図15】 チケット検証の手順を説明するフローチャートである。

【図16】 チケット検証の手順を説明するフローチャートである。

【図17】 チケット検証の手順を説明するフローチャートである。

【図18】 チケット検証の手順を説明するフローチャートである。

【図19】 チケット証明の手順を説明するフローチャートである。

【図20】 チケット証明手順の一部を説明するフローチャートである。

【図21】 チケット証明手順の一部を説明するフローチャートである。

【図22】 チケット証明手順の一部を説明するフローチャートである。

【図23】 チケット証明手順の一部を説明するフローチャートである。

【図24】 チケット証明手順の一部を説明するフローチャートである。

【図25】 チケット証明手順の一部を説明するフローチャートである。

【図26】 チケット証明手順の一部を説明するフローチャートである。

【図27】 チケット証明手順の一部を説明するフローチャートである。

【図28】 検証手順実行手段の構成を示すブロック図である。

【図29】 証明手順実行手段の構成を示すブロック図である。

【図30】 チケット検証器の構成を示すブロック図である。

【図31】 チケット証明手順を説明するフローチャートである。

【図32】 チケット検証の手順を説明するフローチャートである。

【図33】 チケット証明手順を説明するフローチャートである。

【符号の説明】

1 チケット作成・発行装置

2 チケット証明装置

3 チケット検証装置

4 チケット作成手段

5 チケット発行手段

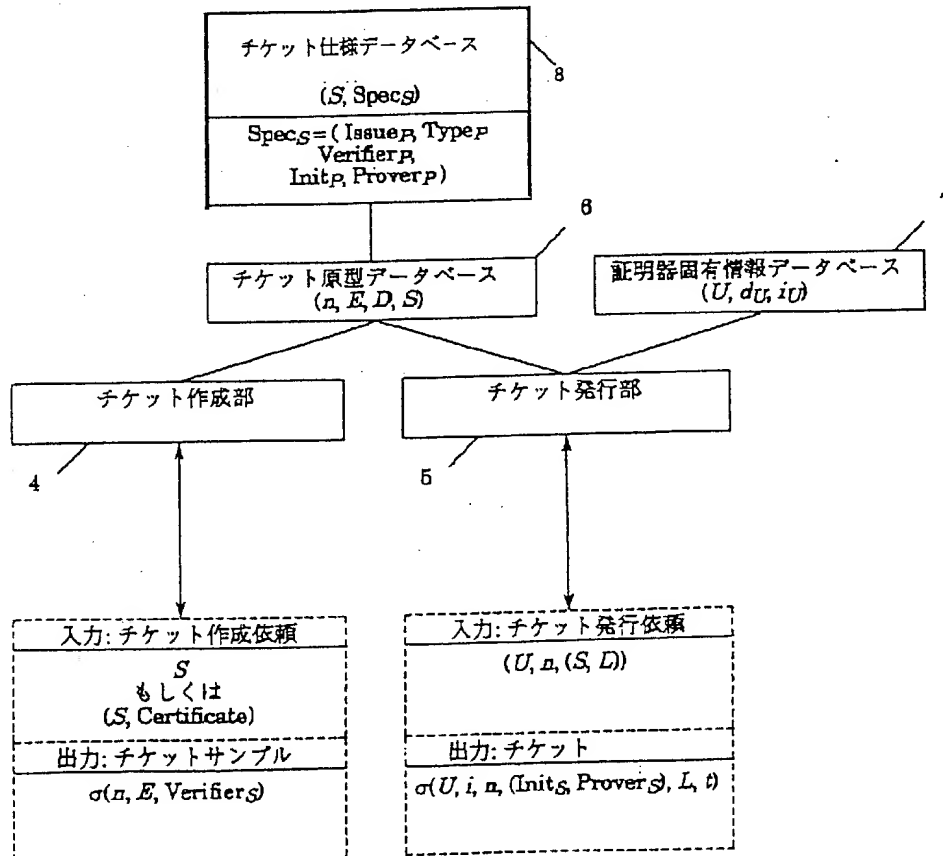
6 チケット原型データベース

7 証明器固有情報データベース

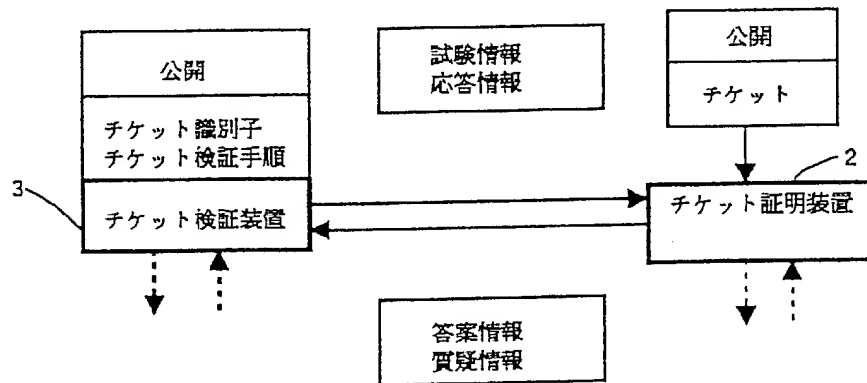
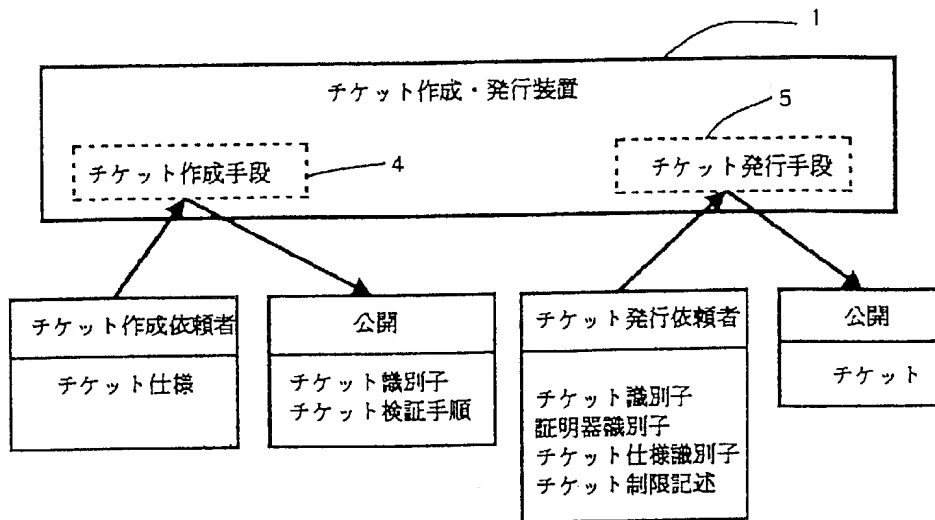
111 検証手順実行部
 112 通信部
 121 チケット保持部
 122 チケット検索部
 123 固有情報保持部
 124 内部状態保持部
 125 証明手順実行部
 126 通信部
 281 検証手順実行部111の送信部
 282 検証手順実行部111の受信部
 283 検証手順実行部111の第1の演算部
 284 検証手順実行部111の第2の演算部
 285 検証手順実行部111の正当性検証部
 286 検証手順実行部111の認証情報生成部
 287 検証手順実行部111の認証情報保持部
 288 検証手順実行部111のチケット識別子保持部
 289 検証手順実行部111の情報保持部
 2810 検証手順実行部111の出力情報保持部

2811 検証手順実行部111の入力情報保持部
 2812 検証手順実行部111の出力部
 2813 検証手順実行部111の入力部
 2814 検証手順実行部111の利用証拠情報保持部
 2814
 291 証明手順実行部125の送信部
 292 証明手順実行部125の受信部
 293 証明手順実行部125の第1の演算部
 294 証明手順実行部125の第2の演算部
 295 証明手順実行部125の正当性検証部
 296 証明手順実行部125の認証情報生成部
 297 証明手順実行部125の認証情報保持部
 298 証明手順実行部125の第2の認証情報保持部
 299 証明手順実行部125の情報保持部
 2910 証明手順実行部125の出力情報保持部
 2911 証明手順実行部125の入力情報保持部
 2912 証明手順実行部125の制御部

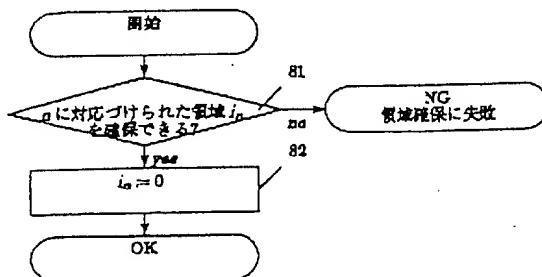
【図3】



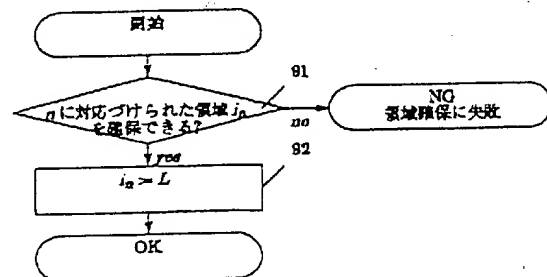
【図1】



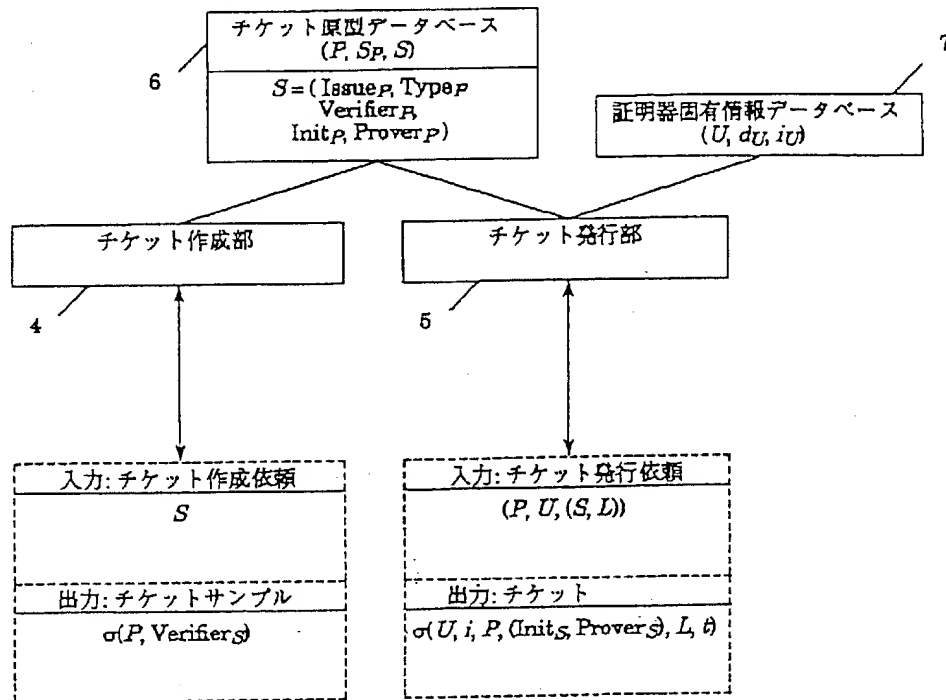
【図8】



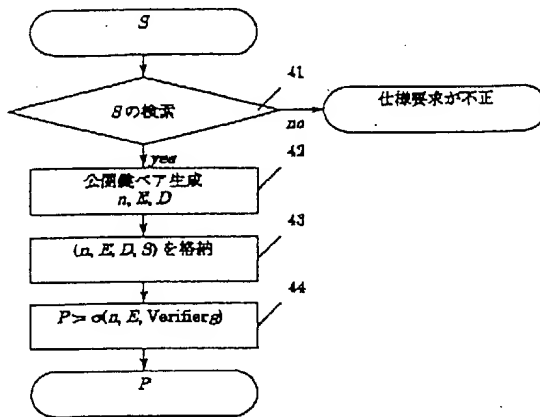
【図9】



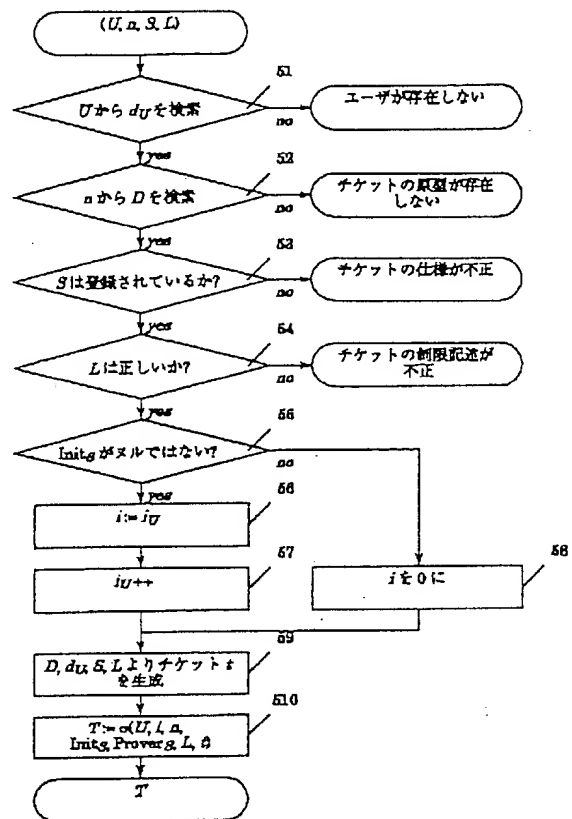
【図 2】



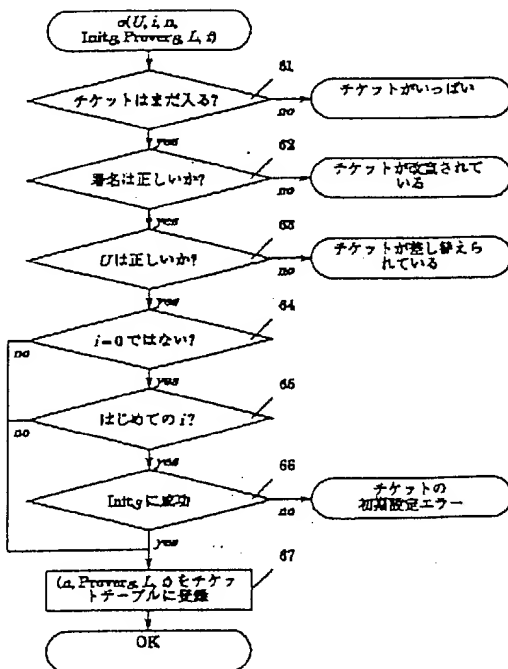
【図 4】



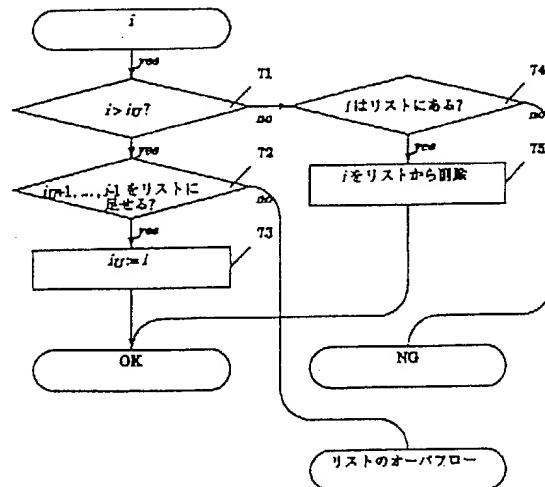
【図 5】



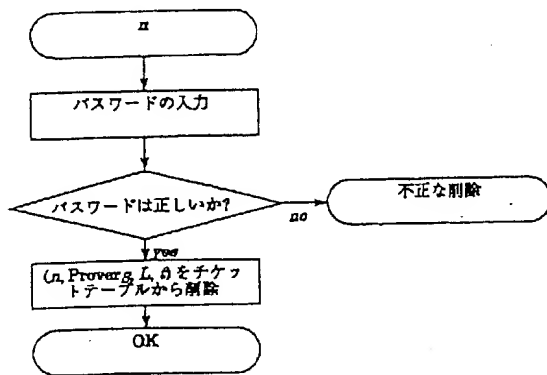
【図 6】



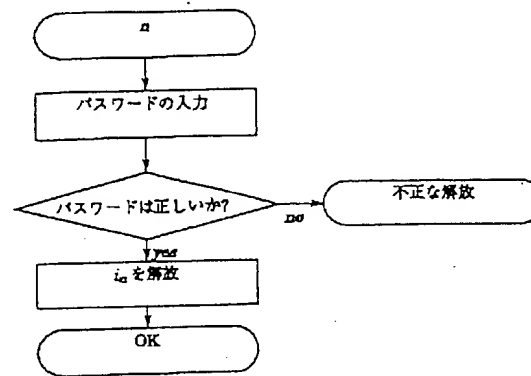
【図 7】



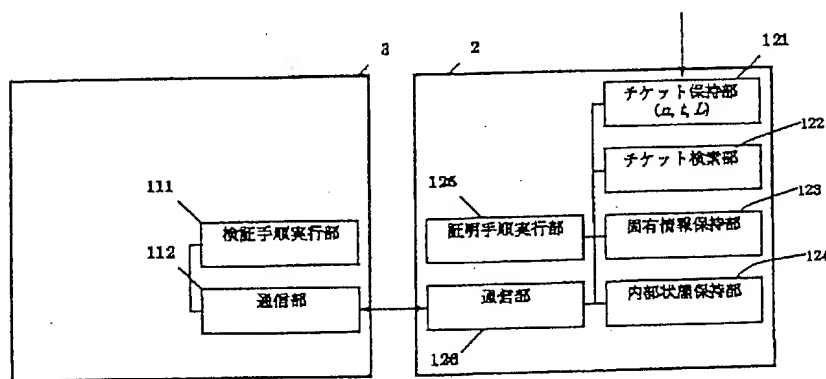
【図10】



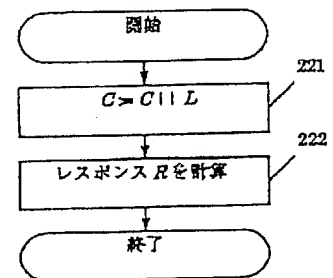
【図11】



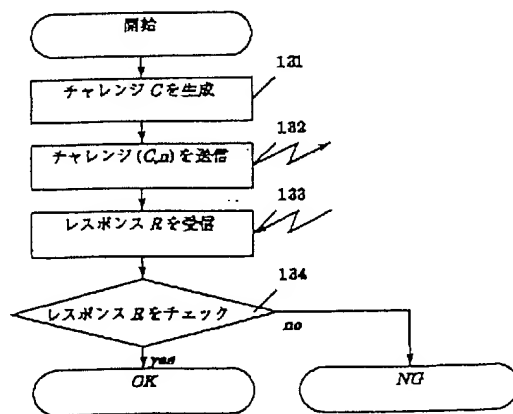
【図12】



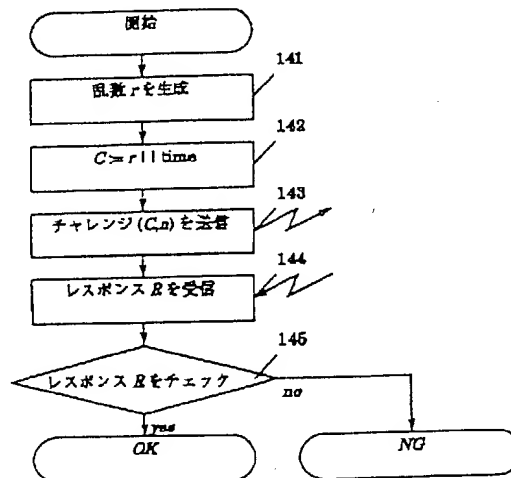
【図22】



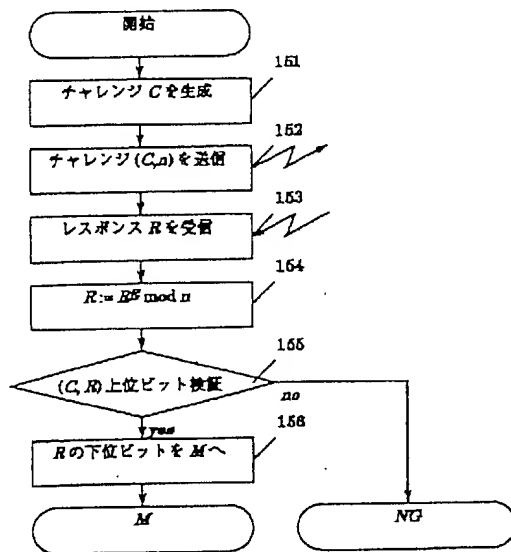
【図13】



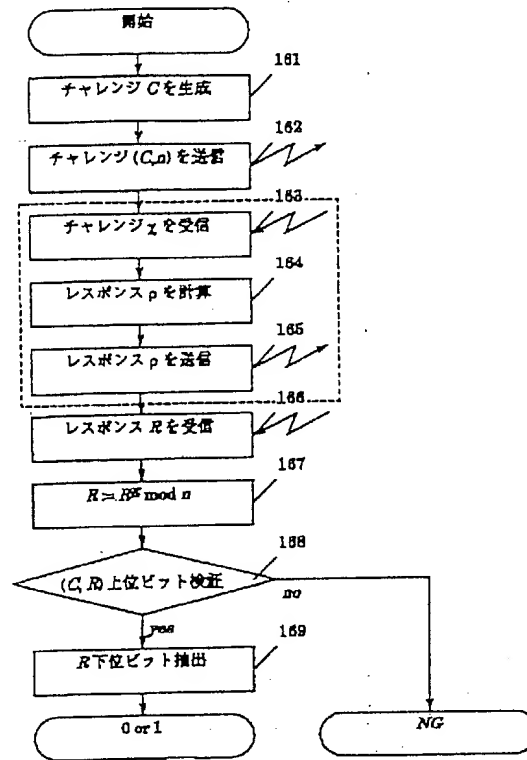
【図14】



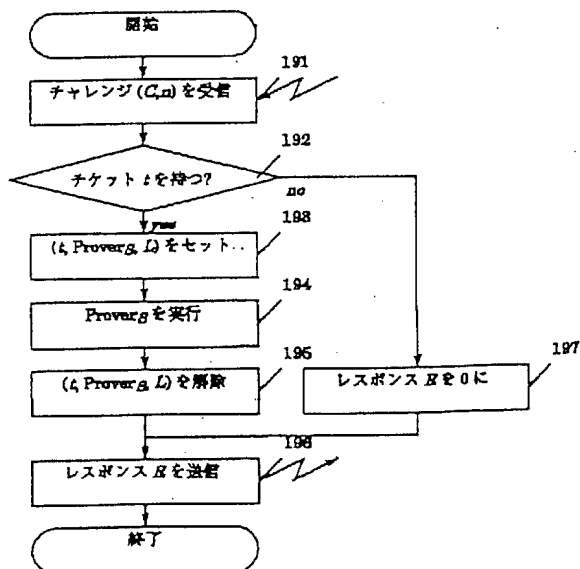
【図15】



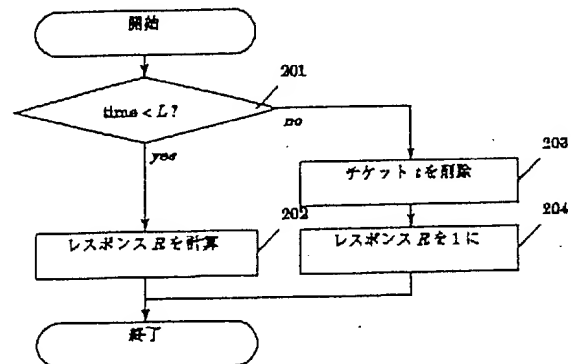
【図16】



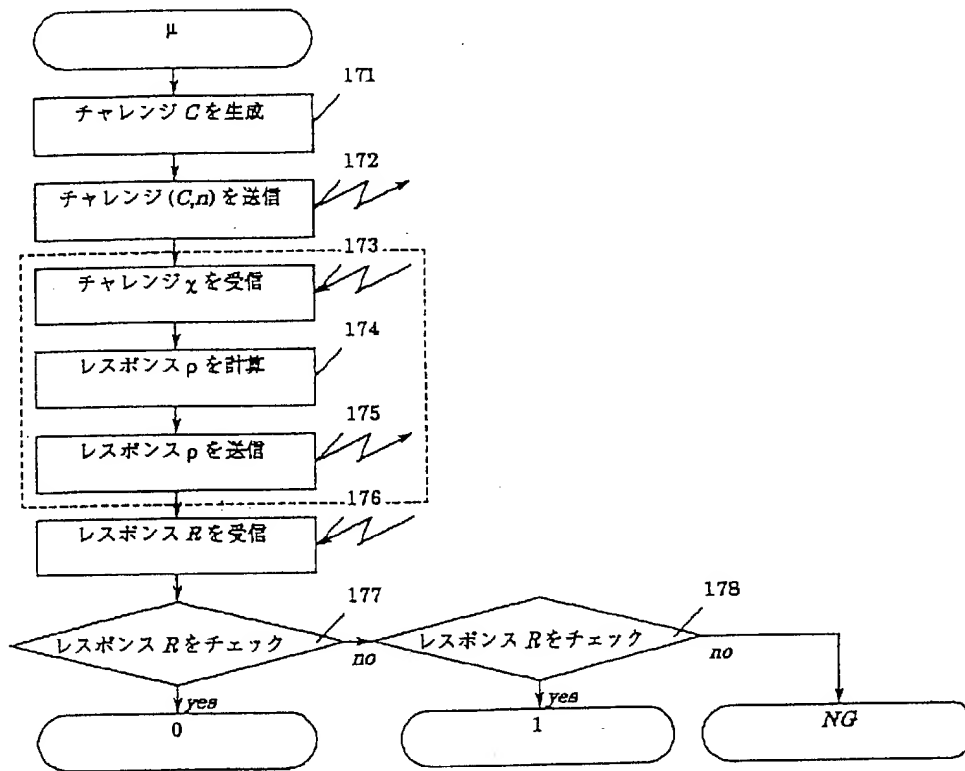
【図19】



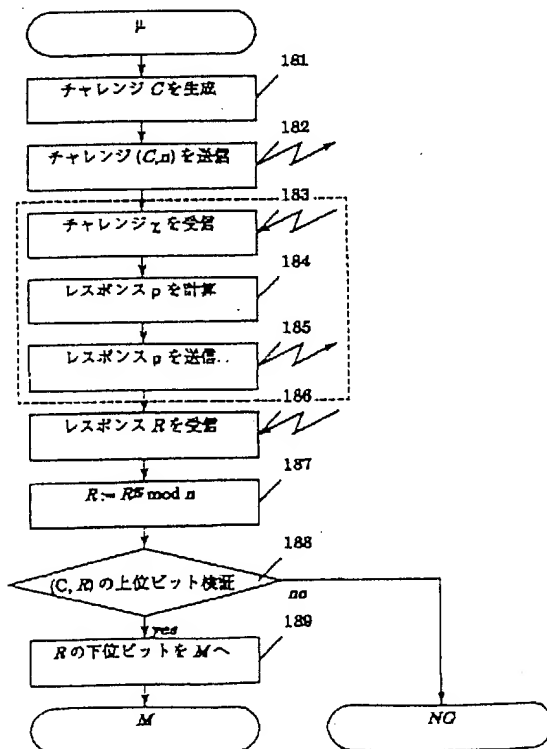
【図20】



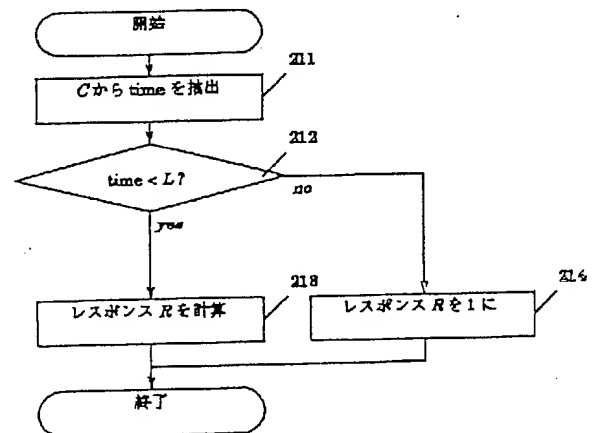
【図17】



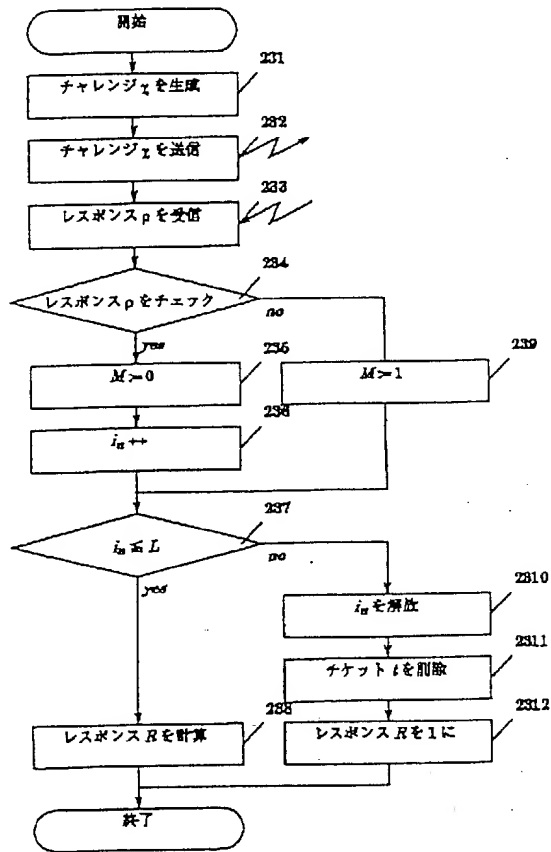
【図18】



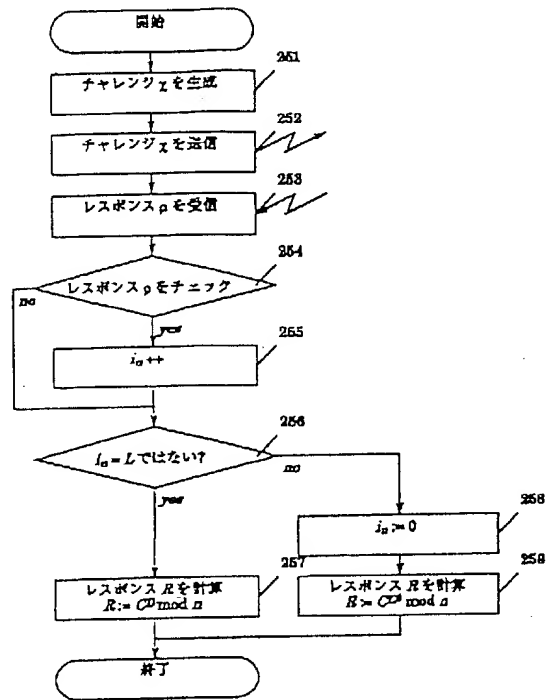
【図21】



【図23】

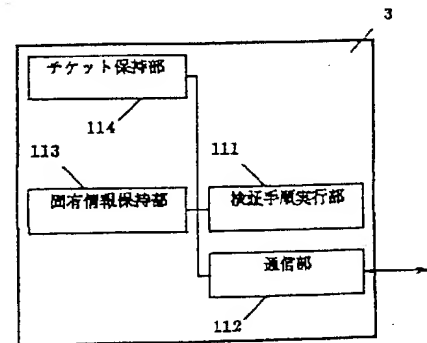
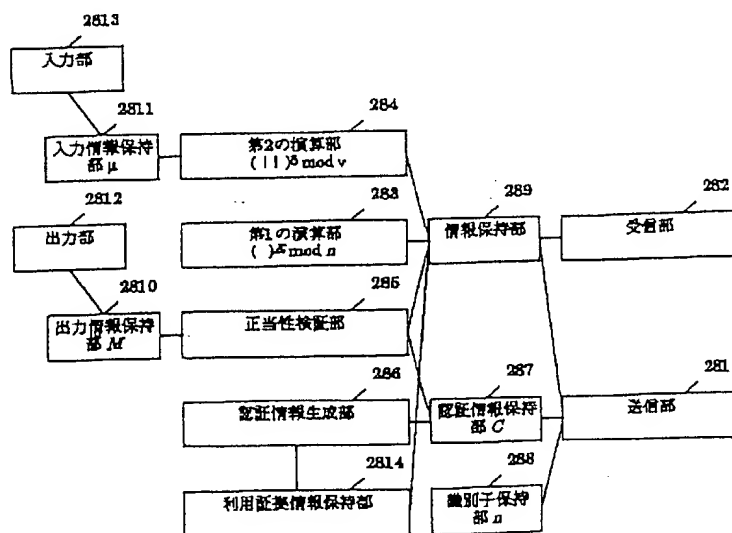


【図25】

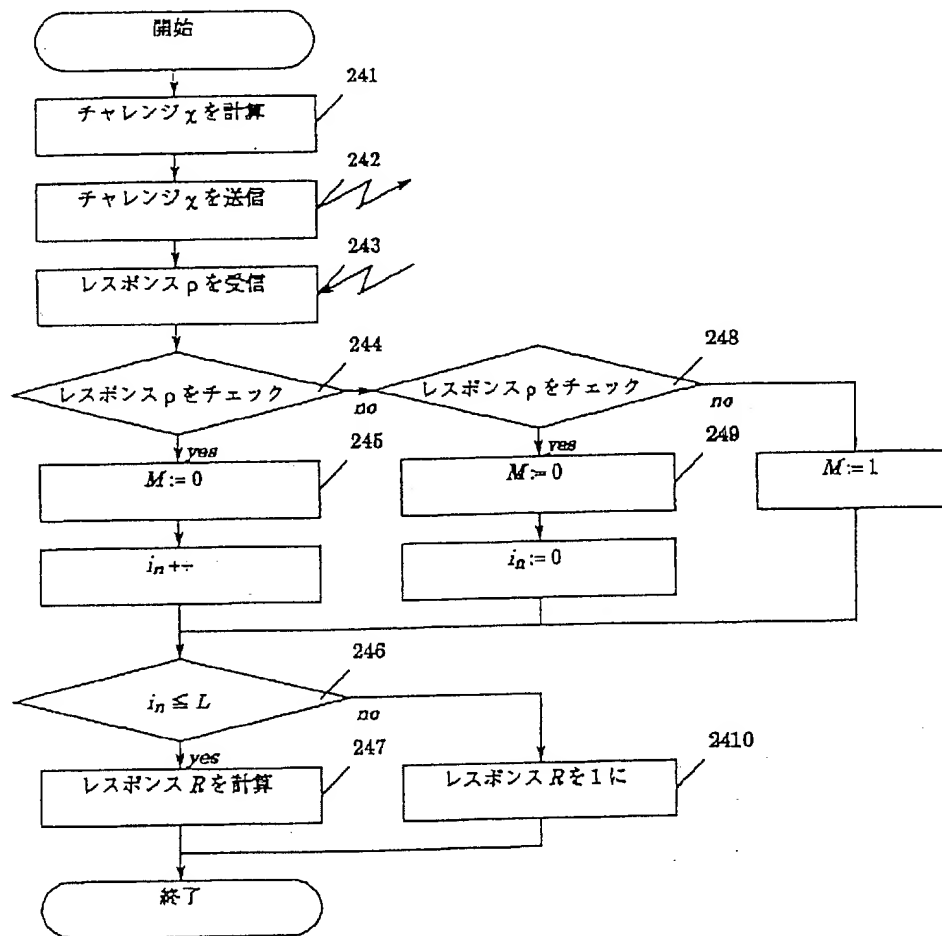


【図30】

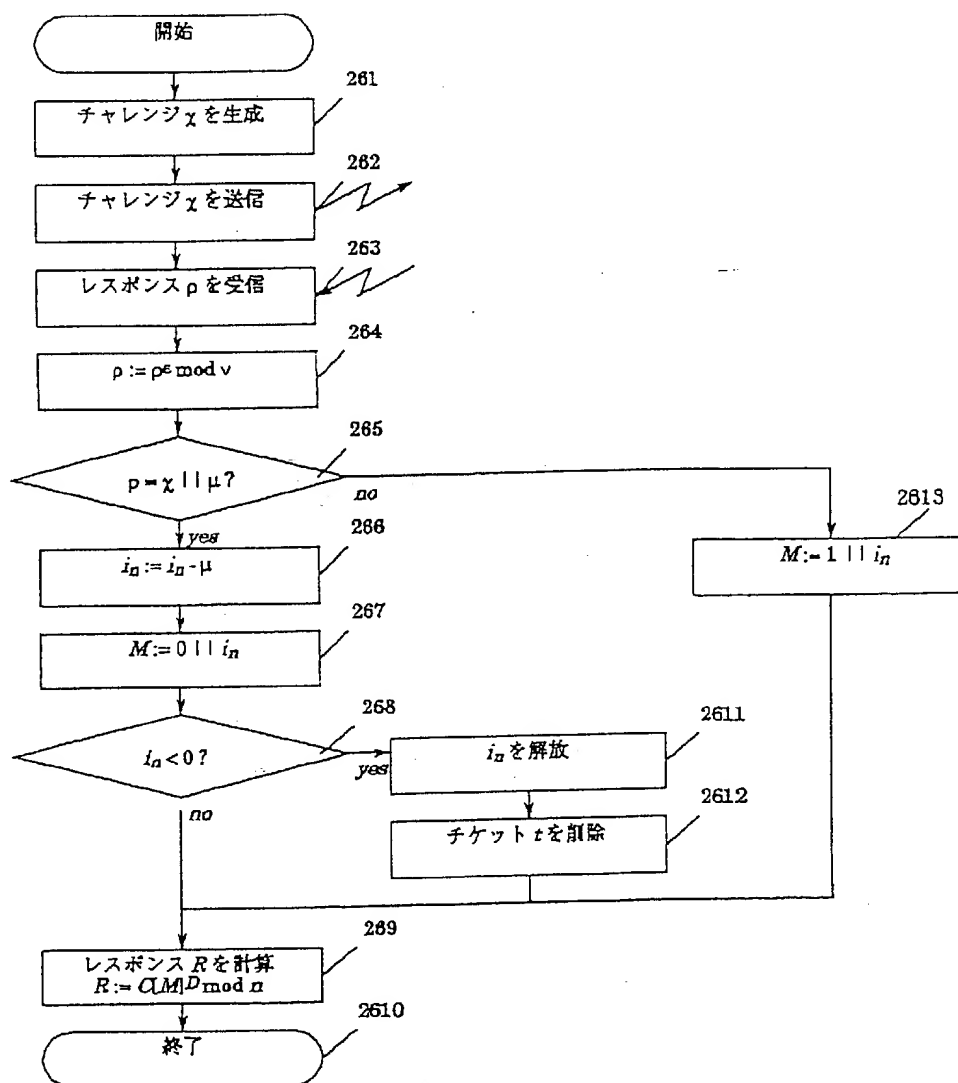
【図28】



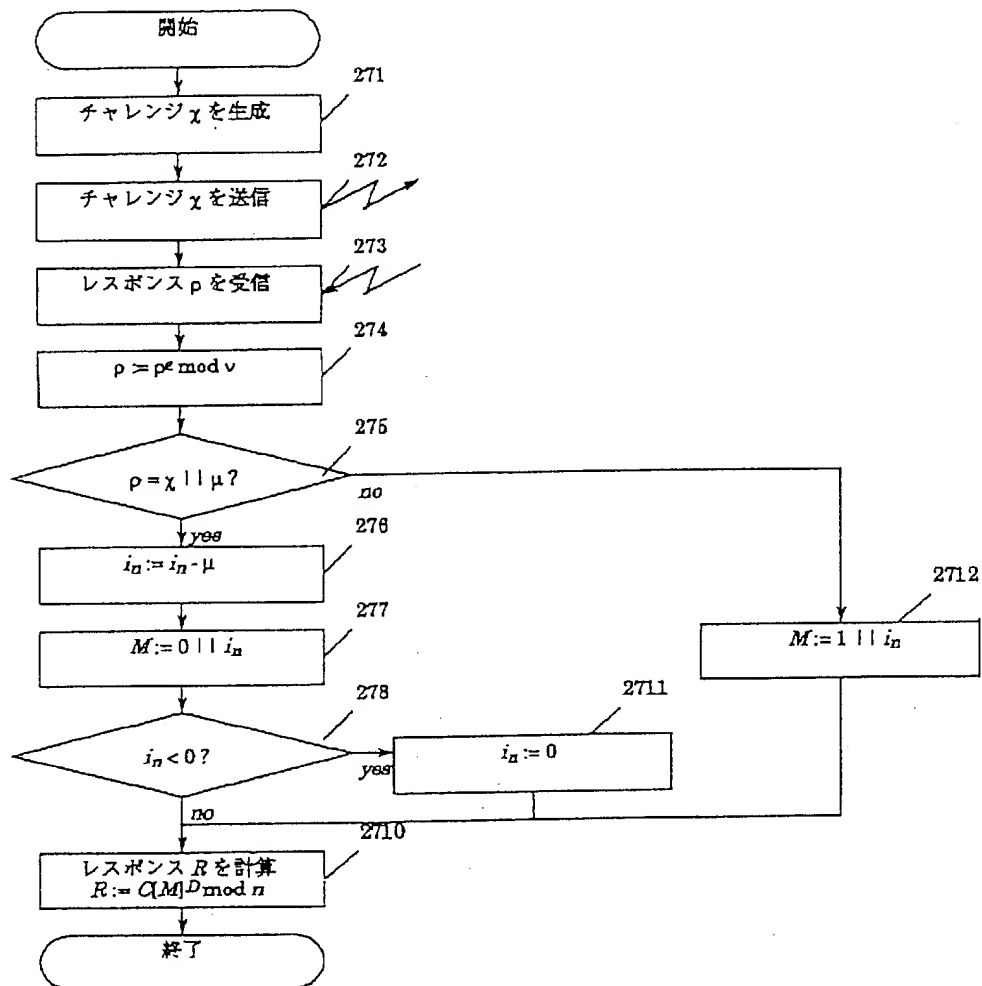
【図24】



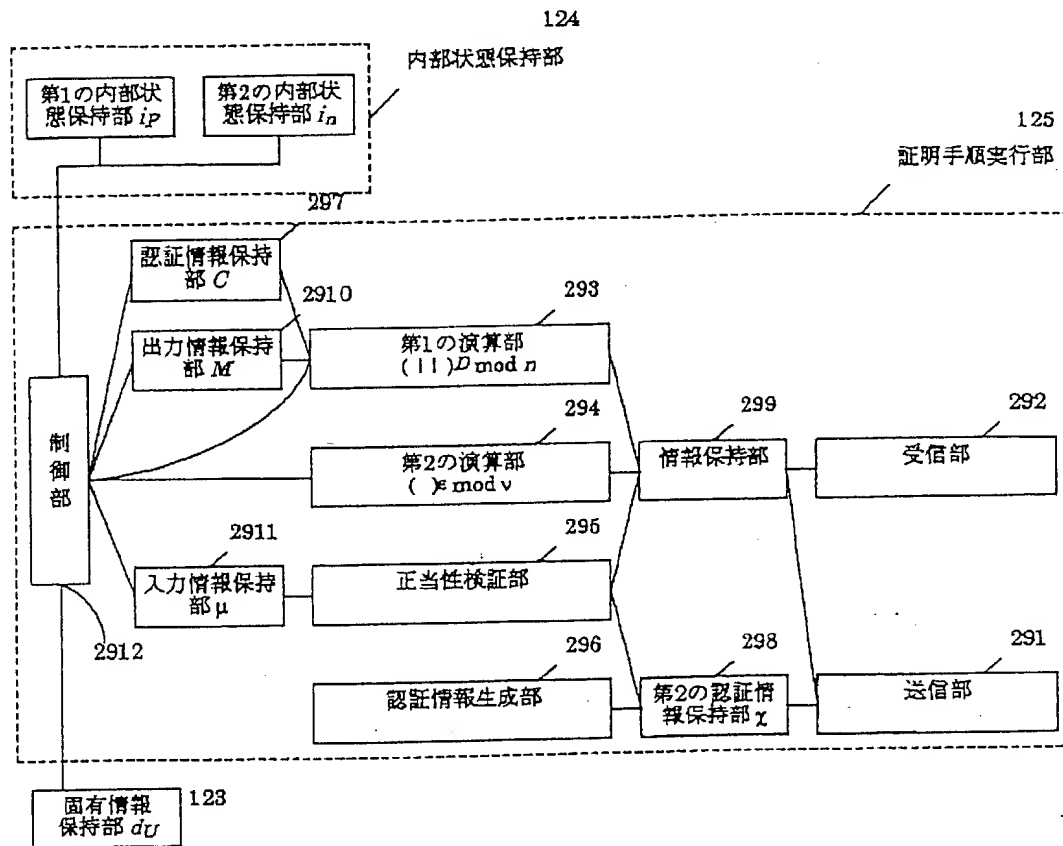
【図 26】



〔図 27〕



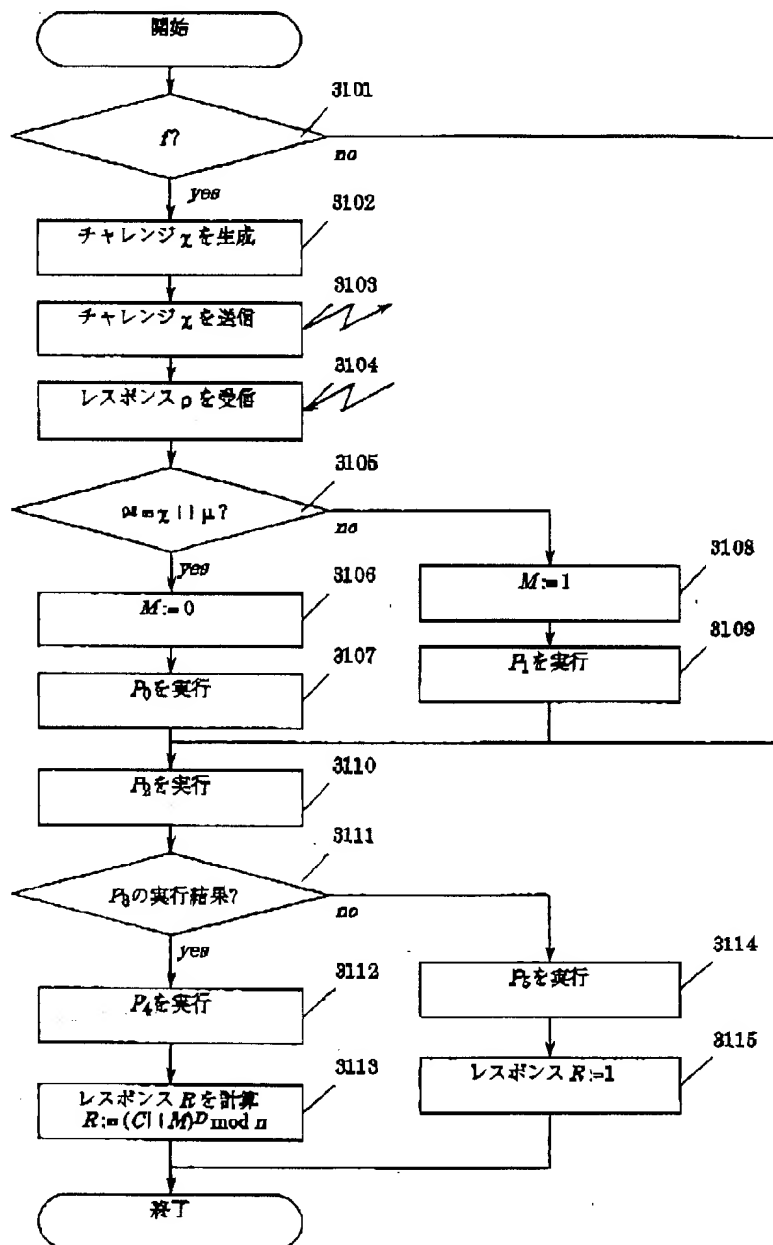
【図29】



(48)

特開平11-31204

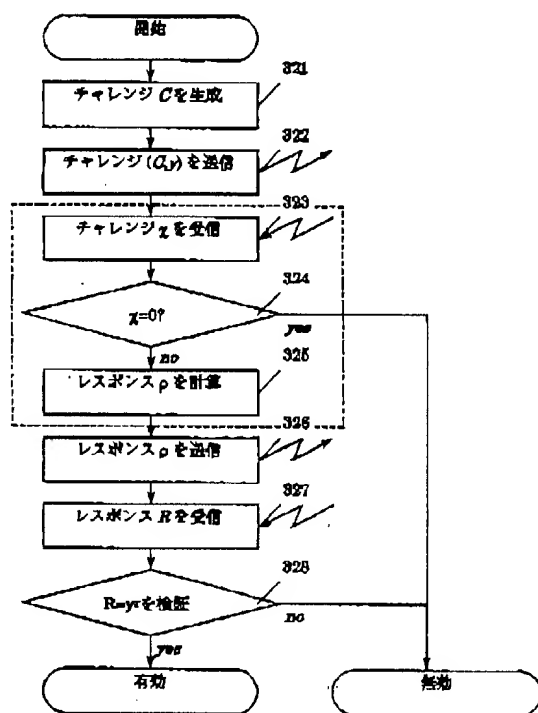
【図31】



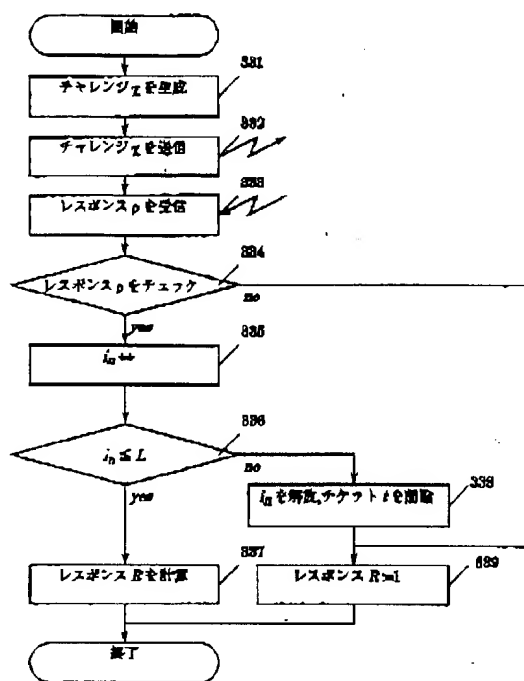
(49)

特開平11-31204

【図32】



【図33】



フロントページの続き

(51) Int. Cl.⁶

H04L 9/32

識別記号

FI

H04L 9/00

675C